WASHINGTON
LEGISLATIVE OFFICE

301887

October 25, 2004

Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
[illegible] STREET, NW, [illegible] FL
WASHINGTON, DC 20005-4707
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

LAURA W. MURPHY
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
NADINE STROSSEN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

KENNETH B. CLARK
CHAIR, NATIONAL
ADVISORY COUNCIL

RICHARD ZACKS
TREASURER

Re: Comments of the American Civil Liberties Union and Privacy International to the Department of Homeland Security Regarding the Proposed Secure Flight Program [Privacy Act of 1974: System of Records; Secure Flight Test Records, TSA-2004-19160, 69 Fed. Reg. 57,345]

These comments are being submitted jointly by the American Civil Liberties Union (ACLU) and Privacy International (PI). We are filing these comments together to express our common concerns with the Secure Flight program, which we believe will ultimately affect not only those living in America but citizens of nations throughout the world.

The ACLU is a nationwide, non-partisan organization of approximately 400,000 members dedicated to protecting the principles of liberty, freedom, and equality set forth in the Bill of Rights in the United States Constitution. For almost 80 years, the ACLU has sought to preserve and strengthen privacy and equality in American life.

Privacy International is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations. PI is based in London, England, and has an office in Washington, D.C. PI has conducted campaigns and research throughout the world on issues ranging from wiretapping and national security, to ID cards, video surveillance, data matching, police information systems, medical privacy, and freedom of information and expression.

The Secure Flight program has been described by officials of the Transportation Security Administration (TSA) and in the current Privacy Act Notice, which provides notice as required under the Privacy Act of 1974 of the establishment of a "system of records" for the purpose of testing the program. Under the program as it is currently conceived, the government will obtain from the airlines the Passenger Name Records (PNR) for all domestic air travelers, and compare those records with watch lists of suspected terrorists maintained by the Terrorist Screening Center (TSC).

Secure Flight is the successor program to the Computer Assisted Passenger Pre-screening System II, or CAPPS II program. While the Privacy Act Notice at issue primarily addresses the testing plans for Secure Flight, the program appears largely to be a modified version of CAPPS II (see chart). We therefore address these comments to the larger plan or concept for this screening program, which clearly lies behind the currently proposed test.

CAPPS II was an unprecedented proposal to conduct routine background checks on everyday travelers. Under the program, the airlines would have collected standardized identifying information from travelers such as date of birth, and checked that data for consistency against commercial data aggregators. The TSA would then have run each passenger through a "risk assessment function" involving unknown secret government information sources, and unknown criteria and algorithms by which that information was judged. Out of that "black box" process, 3-4% of passengers would be labeled as "elevated, uncertain or 'unknown risk'" or "high risk" and treated accordingly.[1]

Secure Flight Compared to CAPPS II

Program elements	CAPPS II	Secure Flight
Provides no protection against terrorists with fake IDs	√	√
Provides no meaningful way for individuals to challenge their security designation	√	√
Centers around reliance on secret, inaccurate government terorrist watch lists		√
Checks personal information against private databases	√	√[2]
Requires collection of personal information from travelers making reservations	√	√[3]
Expands program beyond terrorists	√	
Uses computer algorithms to rate individuals' "threat to aviation"	√	

As with CAPPS II, we continue to lack much of the crucial detail that would be needed to fully evaluate the potential effect of Secure Flight on privacy and other civil liberties. However, clear problems with the proposal remain. We pointed out several of these problems with the CAPPS II proposal, and find that they remain under Secure Flight. They include:

- A failure to be effective
- The inevitability of "mission creep"
- The lack of fair and adequate remedies for affected passengers

[1] See "ACLU Comments to Department of Homeland Security on the 'Passenger and Aviation Security Screening Records,'" September 30, 2003; online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13847&c=206.
[2] TSA officials say that use of commercial databases is merely being "tested" under Secure Flight.
[3] No requirement has been set forth in the current testing phase, but TSA officials say requirement that airlines collect at least full name and date of birth is all but inevitable.

In addition, because of their centrality to the Secure Flight program, we address the many problems that exist with watch lists.

Insecure Flight: This System Will Not Make The Air Travel System Any Safer

One of the criticisms of CAPPS II was that even a known, wanted terrorist could sail right through this system simply by committing identity theft. Nothing in the Secure Flight proposal has changed that hard fact. By committing ID theft (which is all too easy today) and obtaining a false driver's license or passport (which is even easier), a terrorist might present a driver's license with his own photograph, but the name, address, and other information of an innocent person.

A Federal Trade Commission report issued Sept. 3, 2003 reported that nearly 10 million Americans, or nearly 5 percent of U.S. adults, had been victimized by identity theft in 2002. The ACLU conducted its own inquiry and discovered that in less than an hour it was able to purchase online the name, address, phone number, and birth date of volunteers on our staff for less than $50. And once such information was obtained, it would not be hard for a terrorist to put it on a driver's license – even a "real" one – with their own photo. An undercover investigation by the General Accounting Office (made public Sept. 9, 2003) found that it was exceedingly easy to fraudulently obtain a real driver's license by presenting birth certificates and other documents that were intentionally made to be obviously counterfeit.[4]

This system is like a Maginot line – the heavily fortified defensive frontier constructed by the French before World War II, which was rendered useless when Hitler's army simply went around it.

The gaping holes in the security logic behind the Secure Flight proposal are not being acknowledged by the government now, but once this system is put in place, they will inevitably be pointed out by a raft of internal government reports, news articles, and television news exposés.

Ultimately, Secure Flight will not provide a worthwhile security return on the investment required because it will not be backed up by the kind of inviolable, cradle-to-grave national ID database and tracking system that would be necessary to even begin to make if possible to, for example, prevent individuals from obtaining identity documents as imposters. Not only does this nation lack anything resembling such a system, its creation would be – and has been repeatedly judged by the American people to be – highly undesirable due to the privacy violations and government intrusions such a system would bring. Yet, precisely because they would be ineffective without it, creation of identity-based systems such as this program would create strong pressures for the creation of such a system.

---

[4] *See* Fed. Trade Comm'n, *Identity Theft Survey Report* (Sept. 2003), available at http://www.ftc.gov/os/2003/09/synovatereport.pdf; *Counterfeit Identification and Identification Fraud Raise Security Concerns: Hearing Before the Senate Comm. on Finance*, 108th Cong. (September 9, 2003) (Statement of Robert J. Cramer, Managing Director, Office of Special Investigations, U.S. General Accounting Office).

Mission Creep: Security Holes Guarantee Expansion

Once created, Secure Flight will not only lead to pressure for an airtight national identity system, but will inevitably expand itself. That will happen along three separate dimensions:

1. The purposes for which it is used.
Even as a proposal, CAPPS II was expanded from a program that was to focus purely on international terrorists into one that also swept in domestic terrorists and criminals (even as the definition of "domestic terrorist" is expanding). Under Secure Flight, the public is being assured that the program will not be used for anything other than preventing terorrism. But there is no assurance that that policy will last. Once this system is put into place, what reason will its operators give – under the bright glare of the media, perhaps – for refusing to deploy it in the search for a high-profile escaped felon, drug dealer, or other alleged criminal? How long before the system is expanded to flag con-artists, gang members, deadbeat dads, and other suspects? After all, no politician is going to stand up to defend deadbeat dads.

2. The places where it is deployed.
Since the initial proposal of CAPPS II, TSA officials have explicitly indicated that the agency envisions expansion of passenger screening beyond airports to other transportation hubs such as ports. And the 9/11 Commission called for a border security system that "should be integrated into a larger network of screening points that includes our transportation system and access to vital facilities."[5] It is not difficult to anticipate that what begins as Secure Flight will quickly spread to train stations, bus stations, sea ports, "vital facilities," secure office buildings, concert arenas, and so on.

3. The data it draws upon.
The other area in which Secure Flight does appear to represent an improvement over CAPPS II is in the fact that it does not include an automated computerized mechanism for performing "risk assessments" on every passenger. However, as this Notice states, "The Secure Flight test also will involve the use of a streamlined version of the rule set related to suspicious indicators associated with travel behavior" that is used in the existing CAPPS program. The maintenance under Secure Flight of an automated "rule set related to suspicous indicators" raises the prospect that such a rule set could be expanded over time, becoming the functional equivalent of the "risk assessment" proposed under CAPPS II. The Notice's statement that the rule set would be "streamlined" implies that Secure Flight will deploy a subset of the existing CAPPS criteria (which famously include such factors as the purchase of a one-way ticket and cash payment, but also include other, secret criteria) – but also leaves open the possibility for the introduction of new criteria.

Once the government sets down the path of using automated rules for determining "suspicion," those rules will remain a constant, tempting target for expansion, in terms of the sources and amount of data used in the security determination. How much information about a person's life is necessary to conclusively determine that they pose no threat to aviation? Because it is impossible to prove a negative, whatever is collected will never be enough. There will always be security rationales for adding just a little bit more information to the mix.

---

[5] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report: Final Report* (New York, W.W. Norton & Co., 2004), p. 387.

In addition, Secure Flight as currently conceived will make use of the information stores held by "commercial data aggregators who provide services to the banking, home mortgage and credit industries."[6] The stated purpose of using commercial data aggregators is in order to "identify passenger information that is incorrect or inaccurate." Presumably, that would be to protect against anyone simply walking in with made-up information on a false identity card. Of course, as discussed above, even if this proves effective, it still leaves the system utterly vulnerable to imposters who assume the identity of a person whose information in the commercial databases is "in order."

Such gaping holes raise the prospect that the government's reliance on private-sector dossier keepers will also expand over time. The government may well seek to effectively return to the first version of CAPPS II, which would have gone beyond checking whether a passenger's information matched the files of (notoriously inaccurate) credit bureaus and other commercial dossier keepers. It would have sought to measure each passenger's "risk to aviation" by attempting to measure his or her "rootedness in the community" through a full examination of detailed troves of information about each passenger.

In sum, the ineffectiveness of this program and the likelihood that it will undergo mission creep are intimately related. First, this program appears to be moving forward despite gaping holes in the security logic behind it. Second, it is already obvious that the very existence of those security holes will lead to calls for and justifications for the expansion of Secure Flight along numerous dimensions, beginning with a kind of reverse evolution back through the successively more intrusive versions of CAPPS II, and then beyond into an even more expansive program. It is not idle speculation to predict that mission creep of the various kinds discussed here will occur; in each case there are strong logical and historical reasons to believe that it will.

Due process and redress: Who will watch the watch lists?

One of the most serious problems with CAPPS II was that individuals singled out by the program would have had no way of knowing why they were targeted, because the core security evaluations at the heart of CAPPS II were to be completely secret. Secure Flight simply "outsources" the core security determination from mysterious computer algorithms and other unknown criteria, to the equally opaque Terrorist Screening Center (TSC) – and does absolutely nothing to improve the ability of individuals to receive fair treatment when caught up in this system. Innocent victims will not know if they are a victim of the inaccuracies that riddle government and private databases, have been falsely accused of wrongdoing by someone, or have been discriminated against because of their religion, race, ethnic origin, or political beliefs.

There is no doubt that the task facing security agencies is challenging indeed, and we do not object to the idea of trying to identify and keep off aircraft genuine terrorists. But in actual practice, the government's list appears to be so large and bloated that it will inevitably sweep in

[6] In the current phase of the program, this is only being tested. We applaud the effort to actually test a concept before rushing to deployment; however, it is clear that the government is counting on the use of commercial data aggregators to provide some defense against rank invention of names and other identifying material. If Secure Flight's managers allow themselves to conclude that the use of commercial data is too problematic, the system will be left defenseless against anyone walking in with made-up information on a false identity card.

many innocent people (see below), and adequate protections must be built in to deal with the problems that will result.

In a democratic society, the act of maintaining a list of people who are considered suspect and are denied some of the freedoms of others must be scrutinized closely. The power to impose denial of access to common-carrier services such as airlines (which are integral to the free and normal conduct of life for many in today's society) as well as the government's power to stigmatize individuals through the authority and credibility that its designations can hold within a community make it vital that checks and balances be instituted to govern the power to enforce a watch list.

The importance of such checks and balances is made clear by the experience that many Americans have had since 9/11 in their encounters with the TSA's current "no-fly" and "selectee" lists (which restrict individuals from boarding aircraft, or single them out for particularly intense security screening, respectively). Hundreds if not thousands of innocent passengers have been routinely stopped, questioned and searched while trying to fly. Many have been detained and humiliated in front of other passengers.

TSA officials have implied that they have an internal process in place for adjudicating the problems caused by these watch lists. For example, when Senator Ted Kennedy described in a hearing the problems that he himself experienced in getting his name removed from the list, and asked what that implied about the ability of average citizens to do so, DHS undersecretary Asa Hutchison responded that:

> It is important for the average citizen to know the process – that they can call our TSA ombudsman, who will take the information down, verify that they – their name is not the same as what's confusingly similar on the list, and we can actually enter into the database that they have been cleared so that that should be prevented in the future, and so there is a process to clear names.[7]

However, this does not comport with experience. First, individuals who have been repeatedly stopped because their name appears on the no-fly or selectee lists have not consistently been informed of the existence of this ombudsman. Second, those individuals who have discovered it have been instructed to submit to the TSA a written complaint describing in detail the events that occurred. But the TSA states that it will respond to such complaints only if "circumstances warrant it" – with no hint about what those circumstances might be, and no recourse when TSA appears to decide that circumstances do not warrant response. And in fact, many innocent passengers who follow TSA's procedures – filling out forms, providing multiple copies of identification documents, and so on – receive no response from the TSA and continue to be flagged by the No-Fly list.[8]

Even these troubling experiences represent only one aspect of the problem: instances in which individuals not suspected of ties to terrorist organizations are mistaken for other individuals who are. But there are also the cases that arise when an individual is correctly identified as being on a

---

[7] *The 9/11 Commission and Recommendations for the Future of Federal Law Enforcement and Border Security: Hearing Before the Senate Judiciary Comm.*, 108th Cong. (August 9, 2004) (testimony of Asa Hutchison, Under Secretary, Department of Homeland Security).

[8] For more information, see *Michelle Green et al. v. TSA et al.*, Western District of Washington, ACLU class action complaint concerning the no-fly list), available online at http://www.aclu.org/Files/OpenFile.cfm?id=15424.

watch list, but claims that he or she is innocent of ties to terrorist organizations or other allegations and does not belong on the list. (An example of such a case, abeit in the context of an international flight, was the widely publicized detention and expulsion of the Yusuf Islam, the ex-pop star formerly known as Cat Stevens.)

In fact, documents obtained by the ACLU through the Freedom of Information Act (and a lawsuit that had to be filed to force compliance therewith) provide a behind-the-scenes glimpse into the uphill battle that individuals currently face in trying to remove their names from the list. One document states that

> TSA will only remove a name from the No-Fly list if the originator of the request to watch list provides, in writing, a request for the individual to be removed from the list, as well as a sufficient justification for the removal. . . . Additionally, TSA will consider any threat information that other agencies may have presented concerning the individual before deciding whether to remove the person from the No-Fly list."[9]

In short, the current process for seeking redress for watch list problems appears to require that a government agency other than the one administering the list (the TSA) initiate a request for removal, and that such a request not be contradicted by information provided by other agencies (a situation that would presumably require simultaneous self-initiated removal requests from both agencies). Even then, it is up to the TSA to judge, based on unstated criteria and without appeal, whether the justification for removal is "sufficient."

Another document advises FBI field offices that "there have been occasions when agencies have failed to remove names from TSA's lists, even after the individuals were determined by the entering agency to be . . . no threat to commercial aviation." The document then goes on to discuss attempts to remedy this confusion.[10]

The ACLU-obtained documents state that placement on the list is based on whether an individual presents "a threat to U.S. civil aviation," and is sufficiently well identified for their inclusion to be useful. However, it states that these principles are "guidelines, not 'hard and fast' rules," and appears to describe exceptional cases of people placed on the list even though the guidelines would not support such a determination (the precise descriptions of these exceptions were redacted from the documents provided to the ACLU).[11] Clearly, placement on the list is a highly subjective process subject to enormous discretion by invisible, unaccountable security workers.

For an innocent person placed on one of these lists, this all could add up to a situation from which it is, for all practical purposes, impossible to escape.

It is inconceivable that a democratic nation can allow the creation of a vast infrastructure for denying individuals their full freedoms, without tight checks and balances on that machinery. Those checks and balances are well established in other areas where individuals are subject to what amounts to punishment, such as the criminal justice system:

---

[9] *See* No Fly List Document, Exhibit A Part 2, p. 0151, available online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16728&c=282.
[10] See No Fly List Document, Attachment B Part 1, p. 127, available online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16728&c=282.
[11] See No Fly List Document, Exhibit A Part 2, p. 0151, available online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16728&c=282.

- **Meaningful due process.** Individuals must be provided with a meaningful, participatory process by which they can challenge their inclusion on a watch list in an adversarial proceeding before a neutral arbiter.
- **Access to and a right to challenge the data on which inclusion on a list is based.** Before any individuals lose the rights and privileges that other members of society enjoy (such as the right to travel by air) then they must have the same rights to confront their accuser and be told of the charges being leveled against them as individuals currently possess in criminal proceedings. Of course, in some circumstances genuinely justified by true national security imperatives, it may be necessary for data to be reviewed in camera by a neutral arbiter.
- **Tight criteria for adding identities to watch lists.** Security officials must be tightly constrained in their ability to add names to watch lists, and the natural incentive to add a name to a list ("better safe then sorry") must be institutionally counterbalanced.
- **Rigorous procedures for removing names from watch lists.** When the government begins keeping lists of individuals for the purposes of lessening those individuals' freedom, it assumes the responsibility to keep that list up to date by regularly reviewing and reassessing each person's inclusion on that list.

Without such controls, the inevitable result will be a capricious and unpredictable security bureaucracy that will trample on individuals, leaving them no recourse and accepting no accountability.

Proper Management of Watch Lists: Vital But So Far Elusive

Unfortunately, the record of the U.S. government's security establishment in managing its watch lists does not inspire confidence in its ability to do the hard work necessary to institutionalize due process rights. Because of the central role that Secure Flight assigns to watch lists, Secure Flight cannot work if those lists are not managed properly. Yet all evidence indicates that in the years since 9/11 they have been mismanaged:

- Because of the bureaucratic problems and failure to share intelligence that contributed to the 9/11 attack, that disaster prompted security officials to begin seeking to centralize terrorist watch lists.
- In 2002 the General Accounting Office was asked to investigate which federal agencies maintained watch lists and whether watch list information was being shared. In an April 2003 report, the GAO reported a "decentralized and nonstandard" approach to the lists in the government. It uncovered 12 separate watch list systems maintained by 9 federal agencies, and recommended that "the Secretary of DHS take a series of steps aimed at ensuring that watch lists are appropriately and effectively standardized, consolidated, and shared."[12]
- An August 2004 report by the DHS's own Inspector General documents a chain of problems that have bedeviled the government's attempts to create a unified watch list, including the DHS's continued failure to assume responsibility for creating the list, with

[12] General Accounting Office, "Information Technology: Terrorist Watch Lists Should be Consolidated to Promote Better Integration and Sharing," GAO-03-322 (April 15, 2003), available online at http://www.gao.gov/new.items/d03322.pdf.

> the result that responsibility continued to shift among agencies, as well as "an absence of central oversight and a strategic approach to watch list consolidation."[13]

The no-fly documents obtained by the ACLU through the FOIA reinforce the conclusion that the government has failed to properly maintain the watch lists. In one e-mail, an FBI agent, apparently reacting to a TSA official's rationale for the lists, wrote that "Unfortunately, eggheaded thinking like this muddies the waters to the point where the no-fly list and selectee lists become virtually worthless (garbage in, garbage out)."[14] In another e-mail, an FBI agent complained that "These lists are not comprehensive and not centralized. Some subjects appear on one list but not the others. Some of the lists are old and not current. We are really confused."

These documents reveal much confusion and lack of leadership, but they also reveal many good government employees sincerely trying to fix the system and make it more effective at stopping true terrorists. Yet those employees are trapped in a system that is bigger than themselves, and the disastrous experience with the no-fly list has shown the results. But that only serves as a reminder that the danger posed by improperly controlled watch lists is not simply that they will be abused (either by a single "bad apple" or by more systematic, J. Edgar Hoover-style political misuse). There is also the danger that individuals on a list will be bounced around within a Kafkaesque nightmare where no one is responsible, no one is accountable, and no one can help.

The DHS has not even gotten its own house in order on watch lists, and yet is proposing to hurdle forward with the construction of giant machinery that will extend the reach and impact of watch lists outward into everyday American life to an unprecedented degree. The lists at the core of Secure Flight appear to be utterly unready for that role. The result is a danger that Secure Flight will simply serve to throw inaccurate lists at hapless passengers as well as the frontline security personnel who must interact with them and deal with the consequences of bad data.

Focused Watch Lists: Good For Security And Liberty

To be effective, terrorist watch lists must be exactly that: lists focused on true terrorists who pose a genuine threat of taking over or taking down an aircraft. Bloated watch lists are bad not only because they cast many innocent travelers as suspected terrorists, but also because they dissipate the focus that those screeners should be keeping on true terrorists. A terrorist watch list that is discrete and focused has a greater chance of being productive, and a lesser chance of being unfair; not only is it better for civil liberties, but more likely to provide a security benefit. False accusations hassle and humiliate individuals; false positives divert security resources. This is truly a case where good security and civil liberties are aligned.

TSA chief Admiral David M. Stone actually boasted to Congress about the rapidity with which the no-fly list was being expanded, as if that were automatically something good:

> Prior to 9/11, there were fewer than 100 names on the "no-fly" list. Today, TSA provides carriers with "no-fly" and "selectee" lists that have been dramatically expanded. New names

---

[13] DHS Office of Inspector General, "DHS Challenges in Consolidating Terrorist Watch List Information," OIG-04-31, p. 12 (August 2004), available online at http://www.dhs.gov/interweb/assetlibrary/OIG-04-31_Watch_List.pdf. [Hereafter, "DHS IG Report."]

[14] No Fly List Document, Attachment B Part 4, p. 256, available online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16728&c=282.

> are being added every day as intelligence and law enforcement agencies submit new names for consideration. . . . Continued expansion will be possible as integration and consolidation of various watchlists by the Terrorist Screening enter (TSC) progresses. . . [15]

"Continued expansion" of watch lists is not itself helpful, and unless the names being added to the list are of high quality, is likely to be a bad thing. Swamping the names of truly dangerous terrorists in a sea of other names is not good for security. Watch lists become bloated because security workers have every incentive to add names, and no incentives to clear them. Everyday bureaucratic bungling and pure sloppiness is inevitably a factor. But lists can also grow too large because the agencies that maintain them have lost sight of the scope of such lists and the purposes for which they are being maintained. The rapid consolidation of watch lists touted by Stone only reinforces our concern that this is already the case.

Of the 12 watch lists reported by the GAO in its April 2003 report, only one (the State Department's TIPOFF database) was purely a terrorist watch list. The other databases included other information – on violent gangs, individuals suspected of drug trafficking, and other non-terrorist criminals and perceived threats.[16] We do not know how all this extraneous information is being handled as terrorism information is ostensibly being combined into a single repository at the TSC. Consolidation of 12 bloated, inaccurate, out-of-date watch lists would only lead to a single bloated, inaccurate, out-of-date watch list. And it is worrisome that the TSA seems to consider the goal to make these lists as long as possible, rather than to keep them as short and as "threat-rich" as possible. The fact that the TSA's own no-fly and selectee lists are also being added to the TSC database, despite the rampant problems with those lists, further undermines confidence in the composition of the watch list that will lie at the core of Secure Flight.

The attitude that "no potential threat shall go unlisted" leads naturally to bloated watch lists. After all, every single person boarding an airplane is a *potential* threat; for watchlists to have a chance at being effective, they must be created and administered with the discipline to remain focused on terrorists truly intent on taking over or bringing down an airliner.

We worry about reports that there are so many lists, not consolidated, full of extraneous information about people no one would consider a terrorist. The uncontroversial contention that Osama Bin Laden should not be allowed on an aircraft is being used to create and to justify watch lists that appear to be far broader than that image would imply. Secure Flight and the watch list upon which it relies must be confined to a more focused, discrete, and carefully controlled database. If the list sweeps so broadly at the outset, we can only imagine how broadly it will sweep as it becomes susceptible over time to the inevitable mission creep.

Conclusion

We believe that the risks of identity-based systems such as watch lists are high, and their likely security benefits low. We do not object to the concept of checking watch lists for genuine terrorist threats, but the actual implementation of such a list in a free democratic society is fraught with pitfalls. It needs to be fair, and it needs to actually be effective at making our air

---

[15] *9/11 Commission Recommendations on Civil Aviation Security Before the Subcommittee on Aviation of the House Committee on Transportation and Infrastructure*, 108th Cong. (August 25, 2004) (Testimony of David M. Stone), available online at http://www.house.gov/transportation/aviation/08-25-04/stone.pdf.

[16] DHS IG report, 4.

transportation system safer, and not just make people feel better. We are concerned that the TSA is moving headlong toward building this system before ironing out the fundamental problems with the legacy watch list systems on which it would be based. If the agency is to proceed with this system, it should stop to think about the precise contours of its mission, and rethink this program from the ground up. That means:

- Building focused systems that concentrate on alerting screeners to true terrorists who pose genuine threats to aviation safety
- Building carefully bounded systems that will not grow over time into something that brings fundamental new incursions on freedom in America
- Building robust, carefully crafted safeguards with the wisdom that any "Founding Fathers" must possess when they create new institutions that have the potential to threaten liberty.

We appreciate your attention to these comments and please do not hesitate to contact us should you have any questions.

Sincerely,

Laura Murphy, Director
ACLU Washington Legislative Office

Barry Steinhardt, Director
ACLU Technology and Liberty Program

Gus Hosein, Senior Fellow
Privacy International